M. Anderson Berry (262879)
Gregory Haroutunian (330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Alex Straus (321366)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
280 South Beverly Drive
Beverly Hills, California 90212
Telephone.: (917) 471-1894
astraus@milberg.com

Attorneys for Plaintiff

Additional Counsel on Signature Page

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

ANTHONY RUIZ, individually and on behalf of themselves and all others similarly situated,

Plaintiff,

v.

HORIZON ACTUARIAL SERVICES, LLC,

Defendant.

Case No.: 3:22-cv-02279

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Anthony Ruiz ("Plaintiff") alleges upon personal knowledge as to himself and his own actions, and upon information and belief, including the investigation of counsel as follows:

I. INTRODUCTION

1. This action arises out of the recent cyberattack and data breach at Horizon Actuarial Services, LLC ("Defendant" or "HAS") that targeted the information of consumers and other groups who used HAS for actuarial services (the "Data Breach").

2. The Data Breach resulted in unauthorized access to the sensitive data of consumers that used HAS's services. Because of the Data Breach, Plaintiff and Class Members suffered ascertainable losses inclusive of out-of-pocket expenses and the value of their time incurred to remedy or mitigate the effects of the attack and the present and substantial risk of imminent harm caused by the compromise of their sensitive personal information, including their name, date of birth, and Social Security number, and health plan information (hereinafter, the "Personally Identifiable Information" or "PII").

3. HAS's Data Breach occurred on November 10th and 11th of 2021. But HAS sat on the information for over two months – failing to send data breach consumer notifications until January 13, 2022; and then to individuals nearly two months after that on or about March 9, 2022. When a data set that includes this type of PII is breached, every moment is precious to ensure that that data is not weaponized against the rightful owner through identity theft. Sitting on this information allowed HAS to dodge responsibility and worsen the Data Breach victims' chances at weathering the storm that HAS created by not providing adequate protection.

4. As a result of the Data Breach, Plaintiff and Class Members have been harmed and unnecessarily exposed to a heightened present and imminent risk of fraud and identity theft.

5. Plaintiff and Class Members have and may continue to incur out-of-pocket costs, for example, through purchasing credit monitoring services, credit freezes, or other protective measures to reasonably deter and detect identity theft. Plaintiff seeks to remedy those harms on behalf of himself and all similarly situated persons whose PII was unlawfully accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for out-of-pocket costs, and injunctive relief including improvements to

Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

6. As such, Plaintiff brings this Action against Defendant seeking redress for its unlawful conduct, asserting claims for: (i) negligence, (ii) violations of California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. ("CCPA"), (iii) violations of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*., and (iv) declaratory judgment.

II. JURISDICTION AND VENUE

7. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 Class Members and because the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Moreover, Plaintiff, numerous other Class Members, and Defendant are citizens of different states – namely, the Plaintiff is domiciled in California whereas the Defendant is located in Delaware.

8. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operated, conducted, engaged in, or carried on a business in California; committed tortious acts in California; and/or breached a contract in California by failing to perform acts required by the contract to be performed in California.

9. Venue is proper in this district under 28 U.S.C. §§ 1391(a)(1), 1391(b)(1), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this district and Defendant conducts substantial business in this district.

III. PARTIES

10. Plaintiff Anthony Ruiz is a citizen of California, is a plan participant of an entity that utilizes Defendant's services, and received the Notice of Data Breach from Defendant dated March 23, 2022 on or about that date.

11. Defendant Horizon Actuarial Services is a limited liability corporation organized under the laws of Delaware and is headquartered in Delaware.

IV. FACTUAL ALLEGATIONS

DEFENDANT'S BUSINESS

12. According to the Defendant, HAS provides actuarial services throughout the United States; HAS "is a leading consulting firm that specializes in providing innovative actuarial solutions to multiemployer plans."[1]

13. HAS collects confidential data from business entities that utilize its services about individuals (including Plaintiff and Class Members) to provide its services. That sensitive information includes:

a. Name;

b. Address;

c. Email address;[2]

d. Social Security number; and,

e. Health plan information.[3]

14. In its Privacy Policy, HAS states that it "respects privacy" and "[w]e use commercially reasonable administrative, technical and organizational measures to help secure Collected Data against loss, misuse, and alteration."[4] HAS also boasts that it will only share PII "with third parties if we believe it is needed to operate the [website] or to protect our rights or the rights of others, including sharing data needed to identify, contact, or bring legal action."[5]

15. By obtaining, collecting, using and deriving benefits from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting said PII from unauthorized disclosure.

16. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII.

---

[1] https://www.horizonactuarial.com (last accessed Apr. 6, 2022).
[2] https://www.horizonactuarial.com/website-privacy-policy.html (last accessed Apr. 6, 2022).
[3] HAS's Data Breach Notification, available at https://www.horizonactuarial.com/notice-of-data-incident.html (last accessed Apr. 11, 2022).
[4] https://www.horizonactuarial.com/website-privacy-policy.html (last accessed Apr. 12, 2022).
[5] *Id*.

17. Contrary to the Privacy Policy's representation, Defendant failed to respect and protect consumer privacy.

THE DATA BREACH

18. To define data breaches: "a data breach exposes confidential, sensitive, or protected information to an unauthorized person. The files in a data breach are viewed and/or shared without permission."[6]

19. In November of 2021, HAS experienced a security incident involving unauthorized access to its file servers.

20. Defendant HAS launched an investigation and determined that an unauthorized individual obtained access to files on its storage servers from November 10 to November 11, 2021.

21. Then HAS sat on the information for over two months – failing to disseminate data breach consumer notifications until January 13, 2022; and then to individuals nearly two months on or about March 9, 2022.

22. The sensitive PII stolen in the Data Breach included Class Members' names, dates of birth, Social Security number, and, for some, health plan information.

23. The PII contained in the files accessed in the Data Breach was not encrypted or redacted.

24. Plaintiff and Class Members provided their Personally Identifiable Information to Defendant with the reasonable expectation and the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Defendant's data security obligations were particularly important given the substantial increase in data breaches preceding the date of the breach.

25. Therefore, the increase in such attacks, and the attendant risk of future attacks was widely known to the public and to anyone in Defendant's industry, including the Defendant itself.

[6] "*How Data Breaches Happen*," KASPERSKY, at https://www.kaspersky.com/resource-center/definitions/data-breach (last accessed April 12, 2022).

SECURING PII AND PREVENTING DATA BREACHES

26. HAS could have prevented this Data Breach by properly encrypting or otherwise protecting their equipment and computer files containing PII.

27. In its notice letters, HAS acknowledged the sensitive and confidential nature of the PII. To be sure, collecting, maintaining, and protecting PII is vital to virtually all of HAS's business purposes as an actuarial services firm. HAS acknowledged through its conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

THE DATA BREACH WAS A FORESEEABLE RISK OF WHICH DEFENDANT WAS ON NOTICE

28. It is well known that PII, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

29. In 2021, there were a record 1,862 data breaches last year, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[7]

30. Individuals place a high value not only on their PII, but also on the privacy of that data. For the individual, identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.

31. Individuals are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers." There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."

[7] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/.

32. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), HAS knew or should have known that its electronic records would be targeted by cybercriminals.

33. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

34. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite their own acknowledgment of its duties to keep PII private and secure, HAS failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

DEFENDANT, AT ALL RELEVANT TIMES, HAD A DUTY TO PLAINTIFF AND CLASS MEMBERS TO PROPERLY SECURE THEIR PRIVATE INFORMATION

35. At all relevant times, HAS had a duty to Plaintiff and Class Members to properly secure their PII, encrypt and maintain such information using industry standard methods, train its employees, use available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when HAS become aware that their PII may have been compromised.

36. HAS had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, HAS breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

37. Security standards commonly accepted among businesses, and that Defendant lacked, include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

38. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[8] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[9]

39. The ramifications of HAS's failure to keep its consumers' PII secure are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims is likely to continue for years.

THE VALUE OF PERSONALLY IDENTIFIABLE INFORMATION

40. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40

[8] 17 C.F.R. § 248.201 (2013).
[9] *Id.*

to $200, and bank details have a price range of $50 to $200.[10] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120.[11]

41. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

42. Furthermore, trying to change or cancel a stolen Social Security number is no minor task. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

43. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that

---

[10] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed April 11, 2022).

[11] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, *available at*: https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed April 11, 2022).

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed April 11, 2022).

old bad information is quickly inherited into the new Social Security number."[13]

44. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[14]

45. PII can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[15]

46. Given the nature of HAS's Data Breach, as well as the length of the time HAS's systems were breached and the extreme delay in notification to Class Members, it is foreseeable that the compromised PII has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' PII can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

47. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because credit card victims can cancel or close credit and debit card accounts.[16] The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

---

[13] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed April 11, 2022).

[14] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed April 11, 2022).

[15] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.

[16] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, Forbes, Mar 25, 2020, *available at*: https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last accessed April 11, 2022).

48. To date, HAS offered its consumers only two years of identity monitoring services. The offered services are inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

49. The injuries to Plaintiff and Class Members were directly and proximately caused by HAS's failure to implement or maintain adequate data security measures.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

50. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

51. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18]

52. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

---

[17] Protecting Personal Information: A Guide for Business, Federal Trade Commission (2016), *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited April 11, 2022).

[18] *Id.*

53. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

54. Defendant failed to properly implement basic data security practices.

55. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Personally Identifiable Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

56. Defendant was at all times fully aware of its obligation to protect the Personally Identifiable Information of its subjects. Defendant was also aware of the significant repercussions that would result from its failure to do so.

57. Several best practices have been identified that at a minimum should be implemented by companies like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti- malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

58. Other best cybersecurity practices that are standard in the Defendant's industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

59. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center

for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

DEFENDANT'S BREACH

61. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches;

b. Failing to adequately protect consumers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of data breaches, the protection of PII, and the maintenance of adequate email security practices;

e. Failing to comply with the FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act; and,

f. Failing to adhere to industry standards for cybersecurity.

62. Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access HAS's IT systems which contained unsecured and unencrypted PII.

63. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and Class Members also lost the benefit of the bargain they made with Defendant.

HARM TO CONSUMERS

64. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

65. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

66. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

67. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

68. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

69. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[19] The fraudulent activity resulting from the Data Breach may not come to light for years.

70. There may be a time lag between when harm occurs versus when it is discovered, and also between when Personally Identifiable Information is stolen and when it is used.

---

[19] Brian Naylor, "*Victims of Social Security Number Theft Find It's Hard to Bounce Back*," NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about- identity-theft.

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, driver's license numbers, and financial account information, and of the foreseeable consequences that would occur if Defendant's data security system and network was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

72. Defendant knew or should have known about these dangers and strengthened its data, IT, and email handling systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

HARM TO PLAINTIFF

73. On or about March 23, 2022, Plaintiff Anthony Ruiz received notice from Defendant that his PII had been improperly accessed and/or obtained by unauthorized third parties. This notice indicated that Plaintiff Ruiz's PII, including name, date of birth, and Social Security number, was compromised as a result of the Data Breach.

74. As a result of the Data Breach, Plaintiff Ruiz made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; researching credit monitoring and identity theft protection services offered by Defendant; paying an initial $30 fee for Experian credit monitoring services and a monthly fee of the same. Plaintiff Ruiz has spent several hours dealing with the Data Breach, valuable time Plaintiff Ruiz otherwise would have spent on other activities, including but not limited to work and/or recreation.

75. In recent weeks, Plaintiff Ruiz has had multiple inquiries made on his credit reports for loans that he did not submit applications, that he reasonable believes are a result of the Data Breach.

76. As a result of the Data Breach, Plaintiff Ruiz has suffered anxiety as a result of the release of his PII, which he believed would be protected from unauthorized access and

disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his PII for purposes of identity theft and fraud. Plaintiff Ruiz is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

77. Plaintiff Ruiz suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Brown; (b) violation of his privacy rights; and (c) present, imminent and impending injury arising from the increased risk of identity theft and fraud.

78. As a result of the Data Breach, Plaintiff Ruiz anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Ruiz is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ALLEGATIONS

79. Plaintiff brings this Action on behalf of himself and on behalf of all other persons similarly situated (the "Class"). Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All natural persons residing in the United States whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "Nationwide Class").
>
> All natural persons residing in California whose PII was compromised in the Data Breach announced by Defendant on or about March 9, 2022 (the "California Sub-Class").

80. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Also excluded from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

81. **Numerosity**. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of over one hundred individuals whose sensitive data was compromised in the Data Breach.

82. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether the Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Personally Identifiable Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to, during, and after the Data Breach complied with the applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards, as applicable;

e. Whether Defendant owed a duty to Class Members to safeguard their Personally Identifiable Information;

f. Whether Defendant breached a duty to Class Members to safeguard their Personally Identifiable Information;

g. Whether computer hackers obtained Class Members Personally Identifiable Information in the Data Breach;

h. Whether the Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether the Plaintiff and Class Members suffered legally cognizable injuries as a result of the Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether the Defendant's conduct violated the UCL;

l. Whether the Defendant's conduct violated the CCPA;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, and/or injunctive relief;

83. **Typicality.** Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

84. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating Class actions.

85. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

86. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

87. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

88. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

89. The PII of Plaintiff and Class Members was entrusted to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

90. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed or obtained by unauthorized parties.

91. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII entrusted to it involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

92. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiff's and Class Members' information in Defendant's possession was adequately secured and protected.

93. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII belonging to persons who transacted with its former customers that Defendant was no longer required to retain pursuant to regulations.

94. Defendant had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff and the Class's PII, and to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

95. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a mandatory step in obtaining services from Defendant.

96. Defendant was subject to an independent duty, untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

97. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

98. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of adequately safeguarding that PII, and the necessity of encrypting PII stored on Defendant's systems.

99. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's PII, including basic encryption techniques available to Defendant.

100. Plaintiff and the Class had no ability to protect their PII that was in, and remains in, Defendant's possession.

101. Defendant was in a position to effectively protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

102. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession was compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was

necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

103. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully accessed by unauthorized third persons as a result of the Data Breach.

104. Defendant, through its actions and inaction, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class when the PII was within Defendant's possession or control.

105. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

106. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the confidential PII entrusted to it in the face of increased risk of theft.

107. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination the PII entrusted to it.

108. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII belonging to persons who transacted with its former customers, and that Defendant was no longer required to retain pursuant to regulations.

109. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

110. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

111. There is a close causal connection between (a) Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and (b) the harm or risk of imminent harm suffered by Plaintiff and the Class. Plaintiff's and the Class Members' PII was accessed

and exfiltrated as the direct and proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

112. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of businesses, such as Defendant, of failing to implement reasonable measures to protect PII. The FTC Act and related authorities form part of the basis of Defendant's duty in this regard.

113. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the damages that would result to Plaintiff and the Class.

114. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

115. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

116. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

117. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud

and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Plaintiff's and Class Members' PII in its continued possession; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of PII as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

118. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

119. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

120. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is now at an increased risk of identity theft or fraud.

121. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demand actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II

Violations of California's Consumer Privacy Act
Cal. Civ. Code § 1798.100, *et seq*. ("CCPA")
(On Behalf of Plaintiff and the California Sub-Class)

122. Plaintiff and California Subclass Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

123. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access and disclosure. The California Legislature explained: "The unauthorized disclosure of personal information and the loss of privacy can have devastating effects for individuals, ranging from financial fraud, identity theft, and unnecessary costs to personal time and finances, to destruction of property, harassment, reputational damage, emotional stress, and even potential physical harm."[20]

124. As a result, in 2018 the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected. Defendant failed to implement such procedures which resulted in the Data Breach.

125. It also requires "[a] business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party . . . [to] require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(c).

126. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for"

[20] *California Consumer Privacy Act (CCPA) Compliance*, https://buyergenomics.com/ccpa-complience/ (last visited April 11, 2022).

statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

127. Plaintiff and the California Subclass Members are "consumer[s]" as defined by Civ. Code § 1798.140(g) because they are "natural person[s] who [are] California resident[s], as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017."

128. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because Defendant:

a. is a "sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners";

b. "collects consumers' personal information, or on the behalf of which is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information";

c. does business in California; and

d. has annual gross revenues in excess of $25 million; annually buys, receives for the business' commercial purposes, sells or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices; or derives 50 percent or more of its annual revenues from selling consumers' personal information.

129. The PII taken in the Data Breach is personal information as defined by Civil Code § 1798.81.5(d)(1)(A) because it contains Plaintiff and the California Subclass Members' unencrypted first and last names and Social Security numbers, among other information.

130. Plaintiff's and the putative California Subclass Members' PII were subject to unauthorized access and exfiltration, theft, or disclosure because their PII, including name and Social Security number, was wrongfully taken, accessed, and viewed by unauthorized third parties.

131. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiff and the California Subclass Members' PII. Defendant failed to implement reasonable security procedures to prevent an attack on their server or network, including its email system, by hackers and to prevent unauthorized access of Plaintiff and the Class Members' PII as a result of this attack.

132. Plaintiff and the California Subclass seek injunctive or other equitable relief to ensure that Defendant hereinafter adequately safeguards PII by implementing reasonable security procedures and practices. This relief is important because Defendant still holds PII related to Plaintiff and the California Subclass. Plaintiff and the California Subclass have an interest in ensuring that their PII is reasonably protected.

133. On April 8, 2022, Plaintiff provided Defendant with written notice by certified mail of Defendant's violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). If Defendant has not "actually cured" the violation within 30 days thereof, Plaintiff will amend this complaint to pursue statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT III
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiff and the California Subclass)

134. Plaintiff and California Subclass Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 87.

135. The UCL prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

136. In the course of conducting their business, Defendant committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiff and Class Members' PII, and by violating the statutory and common law alleged herein, including, *inter alia*, California Consumer Privacy Act of 2018 (Cal. Civ. Code §§ 1798.100, *et seq*.) and Article I, Section 1 of the California Constitution (California's constitutional right to privacy) and Civil Code § 1798.81.5. Plaintiff and California Subclass Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

137. Defendant also violated the UCL's unlawful prong by breaching contractual obligations created by their Privacy Policies and by knowingly and willfully or, in the alternative, negligently and materially violating Cal. Bus. & Prof. Code § 22576, which prohibits a commercial website operator from "knowingly and willfully" or "negligently and materially" failing to comply with the provisions of their posted Privacy Policy. Plaintiff and Class Members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policies.

138. Defendant also violated the UCL by failing to timely notify Plaintiff and California Subclass Members pursuant to Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII. If Plaintiff and Subclass Members had been notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII and identities.

139. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair" business acts and practices in violation of the UCL in that Defendant's wrongful conduct is substantially injurious to consumers, offends legislatively-declared public policy, and is immoral,

unethical, oppressive, and unscrupulous. Defendant's practices are also contrary to legislatively declared and public policies that seek to protect PII and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws such as the CCPA, Article I, Section 1 of the California Constitution, and the FTC Act (15 U.S.C. § 45). The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

140. Plaintiff and California Subclass Members suffered injury in fact and lost money or property as a result of Defendant's violations of their Privacy Policies and statutory and common law in that a portion of the money Plaintiff and Class Members paid on their behalf for Defendant's products and services went to fulfill the contractual obligations set forth in their Privacy Policy, including maintaining the security of their PII, and Defendant's legal obligations and Defendant failed to fulfill those obligations.

141. The UCL also prohibits any "fraudulent business act or practice." Defendant's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

142. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and their violations of the UCL, Plaintiff and Subclass Members suffered injury in fact and lost money or property as a result of Defendant's unfair and deceptive conduct. Such injury includes paying for a certain level of security for their PII but receiving a lower level, paying more for Defendant's products and services than they otherwise would have had they known Defendant was not providing the reasonable security represented in their Privacy Policy and as in conformance with their legal obligations. Defendant's security practices have economic value in that reasonable security practices reduce the risk of theft of customer's PII.

143. Plaintiff and Subclass Members have also suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent,

immediate and the continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII, (iv) statutory damages under the CCPA, (v) deprivation of the value of their PII for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring financial accounts, and mitigating damages.

144. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiff, therefore, on behalf of himself, California Subclass Members, and the general public, also seek restitution and an injunction, including public injunctive relief prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to modify their corporate culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the PII entrusted to it, as well as all other relief the Court deems appropriate, consistent with Bus. & Prof. Code § 17203.

COUNT IV
Declaratory Judgment
(On Behalf of Plaintiff and the Nationwide Class)

145. Plaintiff and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 144.

146. Defendant owes duties of care to Plaintiff and Nationwide Class Members which require them to adequately secure their PII.

147. Defendant still possess Plaintiff's and Nationwide Class Members' PII.

148. Defendant does not specify in the *Notice of Data Breach* letter what steps they have taken to prevent this from occurring again.

149. Plaintiff and Nationwide Class Members are at risk of harm due to the exposure of their PII and Defendant's failure to address the security failings that lead to such exposure.

150. Plaintiff, therefore, seeks a declaration that (1) each of Defendant's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' personal information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiff and Nationwide Class Members for a period of ten years; and

h. Meaningfully educating Plaintiff and Nationwide Class Members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

VI. PRAYER FOR RELIEF

151. **WHEREFORE**, Plaintiff, on behalf of himself and all Class Members, request judgment against Defendant and that the Court grant the following:

a. For an Order certifying the Class as defined herein, and appointing Plaintiff and their counsel to represent the Class;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and the Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and the Class Members;

c. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personally identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personally identifying information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining Plaintiff and Class Members' personally identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other areas of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personally identifying information, as well as protecting the personally identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel

how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personally identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to adequately educate all Class Members about the threats that they face as a result of the loss of their confidential personally identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and, for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to Class Counsel, and to report any material deficiencies or noncompliance with the Court's final judgment;

d. For an award of damages, including actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

e. For an award of reasonable attorneys' fees, costs, and litigation expenses, as allowed by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this Court may deem just and proper.

VII. JURY TRIAL DEMAND

152. Plaintiff hereby demands that this matter be tried before a jury.

DATED: April 12, 2022

Respectfully submitted,

/s/ M. Anderson Berry

M. Anderson Berry (262879)
Gregory Haroutunian (330263)
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Alex Straus (321366)
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
280 South Beverly Drive
Beverly Hills, California 90212
Tel.: (917) 471-1894
Email: astraus@milberg.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
Email: gklinger@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Avenue NW
Suite 440
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
Email: dlietz@milberg.com

Blake Hunter Yagman*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN, PLLC

100 Garden City Plaza, Suite 500
Garden City, New York 11530
Tel.: 212-594-5300
Email: byagman@milberg.com

**pro hac vice forthcoming*

Attorneys for Plaintiff